INTERNATIONAL STANDARD

ISO/IEC 13888-2

Second edition
2010-12-15

Information technology — Security techniques — Non-repudiation —

Part 2: Mechanisms using symmetric techniques

Technologies de l'information — Techniques de sécurité — Non-répudiation —

Partie 2: Mécanismes utilisant des techniques symétriques

This document is a preview generated by EVS

Reference number
ISO/IEC 13888-2:2010(E)

© ISO/IEC 2010

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

This document is a preview generated by EVS

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2010

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

 © ISO/IEC 2010 – All rights reserved

Contents

Page

This document is provided generated by EVS

© ISO/IEC 2010 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 13888-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 13888-2:1998), which has been technically revised.

ISO/IEC 13888 consists of the following parts, under the general title *Information technology — Security techniques — Non-repudiation*:

— *Part 1: General*

— *Part 2: Mechanisms using symmetric techniques*

— *Part 3: Mechanisms using asymmetric techniques*

This document is a preview generated by EVS

 © ISO/IEC 2010 – All rights reserved

Information technology — Security techniques — Non-repudiation —

Part 2: Mechanisms using symmetric techniques

This document is a preview generated by EVS

1 Scope

The goal of the non-repudiation service is to generate, collect, maintain, make available and validate evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action. This part of ISO/IEC 13888 provides descriptions of generic structures that can be used for non-repudiation services, and of some specific communication-related mechanisms which can be used to provide non-repudiation of origin (NRO) and non-repudiation of delivery (NRD). Other non-repudiation services can be built using the generic structures described in this part of ISO/IEC 13888 in order to meet the requirements defined by the security policy.

This part of ISO/IEC 13888 relies on the existence of a trusted third party (TTP) to prevent fraudulent repudiation or accusation. Usually, an online TTP is needed.

Non-repudiation can only be provided within the context of a clearly defined security policy for a particular application and its legal environment. Non-repudiation policies are defined in ISO/IEC 10181-4.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9798-1:1997, *Information technology — Security techniques — Entity authentication — Part 1: General*

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions*

ISO/IEC 13888-1, *Information technology — Security techniques — Non-repudiation — Part 1: General*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 13888-1 and the following apply.

3.1
cryptographic check function
cryptographic transformation which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output

[ISO/IEC 9798-1]

© ISO/IEC 2010 – All rights reserved